# UNITED STATES DISTRICT COURT
# EASTERN DISTRICT OF WISCONSIN

**IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE DISCLOSURE OF PROSPECTIVE CELL SITE INFORMATION**

**Application No. 5485**
**Case No. 06-MISC-004**

## DECISION AND ORDER

The government sought an order, pursuant to 18 U.S.C. §§ 2703 & 3122, authorizing the disclosure of "cell cite information" for a particular cellular telephone. The magistrate judge to whom the application was presented denied the request, prompting the government to object and seek review by me, the duty district judge. I reject the government's argument and affirm the denial of the application.

## I. BACKGROUND

Cellular telephone networks operate by dividing a geographic area into "cells." Each cell contains a tower that receives and transmits signals to and from the cellular phones in the area. When a cell phone is powered up, it automatically searches for and registers with the tower providing the strongest signal. This occurs even when the phone is not in use. If the user moves from one place to another, the phone may transfer to and register with another tower providing a stronger signal. Cellular telephone companies keep track of this information and, for obvious reasons, the government wants to be able to access it. "By a process of triangulation from various cell towers, law enforcement is able to track the movements of the target phone, and hence locate a suspect using that phone." In re

Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005) (hereafter "S.D. Tex.").

## II. DISCUSSION

### A. Standard of Review

The district court's review of a magistrate judge's decision on a non-dispositive matter is limited to determining whether the order is clearly erroneous or contrary to law. 28 U.S.C. § 636(b)(1); Fed. R. Crim. P. 59(a). For the reasons which follow, the magistrate judge's order in the instant case is not clearly erroneous. Indeed, I would affirm the order even under a de novo standard.

### B. Applicable Statutory Provisions

I note at the outset that the issue is not whether the government can obtain cell cite information. Rather, the issue is the standard it must meet before a court will authorize such disclosure. A review of the applicable statutes shows why this is so.

The government is able to access information related to telephone usage primarily in three ways. First, the government is able to obtain a wiretap, permitting it to listen in on calls to and from the target phone, by demonstrating to a district judge that:

> (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated;
>
> (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
>
> (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
>
> (d) there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the

> commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

18 U.S.C. § 2518(3). Due to the fact that this statute requires the government to satisfy additional burdens not applicable to ordinary search warrants, this type of surveillance has been referred to as a "'super-warrant.'" S.D. Tex., 396 F. Supp. 2d at 751 (quoting Orin S. Kerr, Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't, 97 NW. U. L. REV. 607, 630 (Winter 2003)).

Second, the government may obtain "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication] service (not including the contents of communications)," 18 U.S.C. § 2703(c)(1), upon a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation," § 2703(d). This provision is part of a statute known as the Stored Communications Act ("SCA"), and it imposes an "intermediate" standard on the government. S.D. Tex., 396 F. Supp. 2d at 752.

Third, the government may obtain a court order permitting installation of a "pen register," a device that records the numbers dialed from a target phone, or a "trap and trace device," which records the numbers from which calls are made to the target phone, upon "a certification . . . that the information likely to be obtained is relevant to an ongoing

criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b)(2).[1] This statute requires the lowest quantum of information.

Also relevant to this issue is the law concerning "tracking devices," which are defined as "electronic or mechanical device[s] which permit[] the tracking of the movement of a person or thing." 18 U.S.C. § 3117(b). In order to obtain such a device, the government must meet the probable cause standard for warrants set forth in Fed. R. Crim. P. 41. S.D. Tex., 396 F. Supp. 2d at 752.

The final statute relevant to the analysis is the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"). The primary purpose of the CALEA is to ensure that telecommunications carriers make their equipment capable of providing law enforcement with information to which it is entitled under the statutes relating to electronic surveillance. See S.D. Tex., 396 F. Sup. 2d at 762. As is pertinent here, CALEA provides that:

> (a) . . . a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of–
> . . .
> (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier–
>
> > (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

---

[1]More specifically, "the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided." 18 U.S.C. § 3127(3). The "term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." § 3127(4). Both provisions specifically exclude "the contents of any communication."

> (B) in a manner that allows it to be associated with the communication to which it pertains,
>
> except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).

47 U.S.C. § 1002(a)(2) (emphasis added).

Thus, CALEA specifically forbids the government from obtaining information that may disclose the location of the subscriber "solely pursuant to the authority for pen registers and trap and trace devices." As noted, the cell site information the government seeks will allow it to determine the location of the target telephone's user(s).[2] Therefore, because the government may not rely on solely on the Pen/Trap statute, the question is under what authority may the government access cell cite information. The government contends that the SCA provides the additional authority needed and permits the court to authorize disclosure under that statute's intermediate standard. The magistrate judge

[2]The government contends that the information it seeks (i.e., the originating and terminating cellular tower, a map of tower locations, and the physical address of all cellular towers in the applicable market – commonly referred to as the J-Standard) does not provide precise tracking. Rather, it at best allows the government to discover the general neighborhood the target phone user is in at the beginning and end of a call. Nevertheless, although the government has chosen to limit the instant request, nothing in its statutory argument would forbid it from obtaining triangulation information for the entire call or even when the phone is simply on but not in use. In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, No. 06 Crim. Misc. 1, 2006 U.S. Dist. LEXIS 11747, at *6 (S.D.N.Y. Mar. 2, 2006). Indeed, courts have rejected similarly "narrowed" requests. See, e.g., In re United States, No. H-06-356M, 2006 U.S. Dist. LEXIS 56332, at *33 n.28 (S.D. Tex. July 19, 2006) (collecting cases).

disagreed and, according the government, later approved an application for the same information under the Fed. R. Crim. P. 41 probable cause standard.

Can the government obtain cell cite information under the "specific and articulable facts" standard of the SCA, or must it demonstrate probable cause under the standard applicable to search warrants? I turn now to that question.

**C. Analysis**

The government argues that cell cite information falls squarely within the pen register statute's definition of "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). Because CALEA forbids reliance "solely" on that statute, the government also relies on the SCA, contending that cell site information also constitutes "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)," § 2703(c)(1), and therefore may be accessed on a showing of "specific and articulable facts," § 2703(d). The government contends that the SCA provides the additional authority required by CALEA. Courts have characterized this as a "hybrid" or "dual authority" theory of access. E.g., In re United States, 2006 U.S. Dist. LEXIS 56332, at *32.

The hybrid theory poses several problems. First, it begins from the premise that the Pen/Trap statute is the exclusive mechanism by which it may obtain signaling information such as cell site data. Like the magistrate judge, I agree that cell site information appears to fall within the definition of signaling information. Because this is so, the Pen/Trap statute must be coupled with some other statute due to the restriction contained in CALEA. Id. at *36-37. Otherwise, the argument goes, such information may not be accessed at all.

However, there is no reason why the government could not obtain cell site information under Rule 41 or 18 U.S.C. § 2518.[3] The Supreme Court has held that the greater intrusion of allowing electronic surveillance of conversations necessarily includes the lesser intrusion of a pen register. Id. at *41 (citing United States v. New York Tel. Co., 434 U.S. 159, 170 (1977)). Thus, a warrant issued upon probable cause may also provide the basis for obtaining cell site information, or any other type of information covered by the Pen/Trap statute.[4] The government's claim that, unless the Pen/Trap statute is coupled with some other authority, it may not obtain cell site information is simply wrong.

Second, the language in CALEA providing that information obtained solely under the Pen/Trap statute may not include tracking information does not logically require that the Pen/Trap statute be combined with some other statute (such as the SCA) in order to obtain cell site information. In essence, the government contends that "a pen/trap order is a necessary but insufficient condition for obtaining cell site data." Id. at *47. It reaches this conclusion by placing undue emphasis on the word "solely." As Magistrate Judge Stephen Smith aptly stated:

> The "solely pursuant" phrase leaves open the possibility that a pen/trap order may be neither necessary nor sufficient to obtain such data. Consider the following true statement: "A person cannot practice law in California solely

---

[3]I note that in wire tap applications submitted to me under § 2518 the government has regularly requested, and I have granted, cell site data. Clearly, whatever standard is necessary to obtain cell site data, it may be obtained pursuant to a "super-warrant."

[4]The leading decision accepting the hybrid theory mistakenly held that Rule 41 cannot by itself provide authority because any warrant must necessarily authorize the installation of a pen register, the only device that can capture "signaling information". In re Application of the United States, 405 F. Supp. 2d 435, 441 (S.D.N.Y. 2005). As the Supreme Court has held, authorization of a greater intrusion necessarily authorizes a lesser intrusion.

> pursuant to a law degree." A law degree is not sufficient because additional conditions must be met to obtain a law license, most notably passing the bar exam. But neither is a law degree a necessary condition for obtaining a California law license. California is among a handful of states that permits individuals to sit for the bar exam after a four year period of informal study (sometimes termed "reading law"). Just as a law degree may be one route, but not the only route, to obtain a California law license, so a pen/trap order may be one route, but not the only route, to obtain cell site information. Independent statutory authority (such as Rule 41) may also suffice, and this possibility cannot be ruled out based on a literal reading of the "solely pursuant" clause.

Id. at *48-49.

The legislative history does not place such great emphasis on the word "solely." In fact, the house report on the bill omits such reference entirely: "'Call identifying information obtained pursuant to pen register and trap and trace orders may not include information disclosing the physical location of the subscriber sending or receiving the message, except to the extent that location is indicated by the phone number.'" Id. at *48 (quoting H.R. Rep. No. 103-827(I), 1994 WL 557197, at p. 25 (Oct. 4, 1994)). Thus, there is no reason to believe that CALEA requires the coupling of the Pen/Trap statute with the SCA or any other statute, as opposed to requiring the government to make its request under Rule 41 or § 2518.

Indeed, it appears to me that cell cite information, in addition to perhaps constituting "dialing, routing, addressing, or signaling information" under the Pen/Trap statute,[5] could just as easily be covered by the tracking device statute. That statute covers electronic or

[5]One court has noted that, according to the legislative history, "dialing, routing, addressing and signaling information" was intended to cover e-mail and other internet traffic. S.D. Tex., 396 F. Supp. 2d at 761 (citing 147 Cong. Rec. S11006-07 (Oct. 25, 2001) (statement of Sen. Leahy); 147 Cong. Rec. H7197 (Oct. 23, 2001) (statement of Rep. Conyers)).

mechanical devices that permit "the tracking or the movement of a person or thing." 18 U.S.C. § 3117(b). It is true that a cell phone is not like a "bug" attached to a suspect's car, but § 3117(b) is not limited to such devices; under the statute, "it is enough if the device merely 'permits' tracking." S.D. Tex., 396 F. Supp. 2d at 753. If the government is granted access to cell site information, a customer's cell phone will most certainly permit tracking of his movements from place to place. The statute does not require precise tracking, In re United States, 2006 U.S. Dist. LEXIS 56332, at *59-60, so the fact that a cell phone will not permit the government to determine what room of a house the user is in is irrelevant. It is undisputed that cell site data will permit the government to track a person's movements. See S.D. Tex., 396 F. Supp. 2d at 753-54; see also United States v. Forest, 355 F.3d 942, 947 n.10 (6th Cir. 2004), vacated on other grounds, 543 U.S. 1100 (2005) (discussing how the DEA used cell site data to track the suspect's movements). "While the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data." S.D. Tex., 396 F. Supp. 2d at 754.[6]

[6]It is doubtful that the government's use of cell site information to track a suspect implicates the Fourth Amendment, requiring use of the probable cause standard as a constitutional matter. See United States v. Karo, 468 U.S. 705, 714 (1984); United States v. Knotts, 460 U.S. 276, 281-82 (1983); Forest, 355 F.3d at 950-51. However, the issue before me is primarily one of statutory rather than constitutional interpretation. It is plain that the Pen/Trap statute alone does not allow access to such information. It also seems plain that Congress did not give specific consideration to this issue. My task is to decide, given the hierarchy of burdens imposed on access to telephone information, whether the SCA or Rule 41/§ 3117(b) provides the more logical alternate source of authority. I find Rule 41 more apt. This interpretation also has the virtue of avoiding possible constitutional problems if the Supreme Court were to decide that cell site tracking implicates the Fourth Amendment. See In re United States, 2006 U.S. Dist. LEXIS 56332, at *59-61; S.D. Tex., 396 F. Supp. 2d at 757, 765.

Thus, although the government denies that cell site information is akin to a "tracking device" under § 3117(b), it seems clear that the effect is the same. "A Rule 41 probable cause warrant was (and is) the standard procedure for authorizing the installation and use of mobile tracking devices." S.D. Tex., 396 F. Supp. 2d at 752 (citing United States v. Karo, 468 U.S. 705, 720 n.6 (1984)). I also note that revised Fed. R. Crim. P. 41(e)(2)(B), scheduled to go into effect December 1, 2006, expressly covers tracking devices. In re United States, 2006 U.S. Dist. LEXIS 56332, at *57–58. For all of these reasons, I find that cell site information should be obtained under Fed. R. Crim. P. 41 and § 3117(b), or § 2518, rather than the Pen/Trap statute coupled with the SCA. Additionally, I find unpersuasive the government's contention that the SCA, coupled with the Pen/Trap statute, provides adequate supplemental authority.

First, cell site information does not appear to fall within the purview of the SCA. The government fails to demonstrate, by reference to legislative text, history or purpose, that cell site information constitutes "information" or a "record" under the SCA. Even if cell cite data is "information" or a "record" held by a provider, I cannot conclude that the information pertains to a subscriber of an "electronic communication service." Under 18 U.S.C. § 2510(15), "'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications." The statute defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include . . . any communication from a tracking device." 18 U.S.C. § 2510(12). Because "[r]eal-time location monitoring effectively converts a cell phone into

a tracking device," S.D. Tex., 396 F. Supp. 2d at 759, cell site data communicated from a cell phone does not constitute an "electronic communication" under the statute. Cell site information is also not a "wire communication" because "it does not involve the transfer of the human voice at any point along the path between the cell phone and the cell tower." Id.

Second, the structure of the SCA cuts against the government's argument. As its name implies, the statute is concerned with "stored communications" rather than real-time data that will assist in ongoing surveillance. Id. at 760. In other words, the SCA is retrospective rather than prospective. Statutes that permit prospective gathering of information, such as the Wiretap Act and the Pen/Trap statute, contain provisions limiting the length of surveillance, requiring periodic reporting, and providing for the sealing of court records, provisions entirely absent from the SCA. Id. In sum, the SCA pertains to the production of existing records, not information that will be created in the future related to future communications. Id.

Third, the SCA generally forbids the disclosure of subscriber information "to any governmental entity." 18 U.S.C. § 2702(a)(3). There are certain exceptions to the general prohibition on such disclosure, "but not one of those exceptions mentions the Pen/Trap Statute." In re United States, 2006 U.S. Dist. LEXIS 56332, at *53.[7]

> The necessary effect of this omission is to preclude the very authority law enforcement seeks. Section 2702(a)(3) prohibits a phone company from turning over subscriber information "to any governmental entity" except under specified circumstances. None of those circumstances include a pen/trap

[7]Section 2703(c) lists the methods by which a governmental entity may obtain such information, including by obtaining a warrant under the Federal Rules of Criminal Procedure, but it does not refer to a pen/trap order. Id. at *53-54.

> order. If hybrid proponents are correct that a pen/trap order is an indispensable condition for obtaining cell site data, then the SCA by its very terms cannot authorize such disclosure. The dual theory thus self-destructs, its initial premise at war with its intended conclusion.

Id. at *55.

Fourth, the pairing of the Pen/Trap statute and the SCA – which were enacted at different times (as was CALEA) – is not mentioned in any statute or specifically discussed in the legislative history. Id. at *56.

> The Pen/Trap Statute does not mention the SCA or CALEA; SCA § 2703 does not mention CALEA or the Pen/Trap Statute; and the CALEA proviso does not mention the SCA. CALEA does refer to the Pen/Trap Statute, but only in the negative sense of disclaiming its applicability. Surely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way. This is especially so given that no other form of electronic surveillance has the mixed statutory parentage that prospective cell site data is claimed to have.

S.D. Tex., 396 F. Supp. 2d at 764-65 (footnote omitted). Further, FBI Director Freeh, in his testimony in support of CALEA denied "that the SCA had any relevance to CALEA's law enforcement assistance provisions, and the statement of CALEA's House sponsor describ[ed] the final bill as 'plac[ing] limits on the ability of law enforcement to use portable phones as tracking devices.'" In re United States, 2006 U.S. Dist. LEXIS 56332, at *56 (quoting 140 Cong. Rec. H10773-02, 1994 WL 545775 at p. 36 (statement of Rep. Edwards) (emphasis added)).[8]

---

[8]The government notes that the version of CALEA eventually enacted differed from that discussed by Director Freeh. Of significance, the final version contained the words "solely pursuant," which were not suggested by Freeh. As discussed above, I believe that the government places more weight on these two words than they are able to bear. The government also notes that the final version of CALEA made changes to the SCA, including the addition of the new intermediate standard for acquiring information. Still, there is no clear indication in the statute or the legislative history that the SCA and its

To date, most courts which have considered this issue have held that the government must meet the probable cause standard to obtain cell site information and have rejected the government's hybrid theory. See, e.g., In re Order Authorizing Installation and Use of Pen Register, 439 F. Supp. 2d 456, 456 n.2 (D. Md. 2006) (collecting cases); In re United States Application for an Order: Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, No. 1:06-MC-7, 2006 U.S. Dist. LEXIS 45643, at *13 (N.D. Ind. July 5, 2006) (collecting cases); In re Application of United States, No. 06 Crim Misc 01, 2006 U.S. Dist. LEXIS 11747, at *2 (S.D.N.Y. Mar. 2, 2006) (collecting cases). I join these courts and accordingly affirm the decision of the magistrate judge.

## III. CONCLUSION

**THEREFORE, IT IS ORDERED** that the government's appeal is **DENIED**, and the magistrate judge's decision is **AFFIRMED**.

Dated at Milwaukee, Wisconsin, this 6th day of October, 2006.

/s Lynn Adelman

LYNN ADELMAN
District Judge

---

standard were to apply to cell site information. It appears to me that CALEA's limitation on the use of pen/trap orders to acquire tracking information, and its later revision of the SCA, may have been unrelated. The vague comments from Senator Leahy and Representative Edwards quoted by the government do not directly address the issue before me.